

2018 / 4 / 26

الوقت

النظرية الثانية - الخلية

$$(1) \quad ax \equiv b \pmod{m}$$

تبرهن: التماثل الخطي لمعادلة هذه الشكل

حيث a, b أعداد صحيحة معدومة $\exists Z$ عدد صحيح موجب كبير بما فيه $(a, m) \in \mathbb{Z}$ $x \in \mathbb{Z}$ مجهول نبحث عنه (إذا كان لابد من مكان لإبداءه)

هذا التماثل هو المبدأ المنطقي $x \in \mathbb{Z}$ تحقق هذا التماثل.

$$\text{نفرض أن } x \text{ حل للتماثل} \Leftrightarrow m \mid (ax_0 - b)$$

$$\Leftrightarrow \exists y \in \mathbb{Z} \text{ و } my = ax_0 - b$$

$$\Leftrightarrow b = ax_0 + (-m)y \quad (2)$$

وهذه عبارة عن عبارة ديوفانتية (ديوفانتية).

أي أن مسألة حل التماثل الخطي تحول إلى مسألة حل عبارة ديوفانتية.

ملاحظة تعتبر الحلول للتطابقة بالمقام m للتطابق الخطي حلاً واحداً

$$3x \equiv 9 \pmod{12}$$

عند الحل

$$\left. \begin{array}{l} x = 3 \\ x = -9 \end{array} \right\} \begin{array}{l} \text{هذه التطابقات} \\ \text{هي تكافئ 3 فيهما حل واحد} \end{array}$$

$$(9 + (-3) + (-27) = (-3) + (-27) = -30 \pmod{12} = (-3) + (-27) = -30 \pmod{12} = -6 \pmod{12} = 6 \pmod{12})$$

لذلك نرى بعد الحل للتطابق الخطي (1) عدد الحلول غير متطابقة بالمقام m .

وبما أن حل التماثل (1) يكافئ حل معادلة ديوفانتية (2)

وكما علم أن (2) لها حلول إذا وفقط إذا كان القاسم المشترك الأكبر

$$d(a, -m) = d(a, m) \text{ يقسم } b.$$

$$ax \equiv b \pmod{m}$$

يكون للتطابق الخطي

$$\text{حل إذا وفقط إذا كان } d(a, m) \text{ يقسم } b$$

$$d = d(a, m) \mid b$$

وعندئذ يوجد للتطابق عدد d من الحلول المختلفة (غير متطابقة) بالمقام m يعطى بالعلاقة التالية:

$$x = x_0 + \frac{m}{d}t \quad (t = 0, 1, 2, \dots, d-1)$$

نتيجة إذا كان $d(a, m) = 1$ و a, m أوليان فيما بينهما

فالتطابق الخطي المعطى حل واحد

الموضوع:

1 /

$$15x \equiv 60 \pmod{20}$$

مثال

$$d(15, 20) = 5 \mid 60$$

تلاحظ أن

يعيد حلول التقاطع المعطى ويعددها و طول في متلازمة (مختلفة) المتكافئة 20
 لإيجادها، نقسم المعادلات على $d=5$ نحصل على تطابق آخر.

$$3x \equiv 12 \pmod{4}$$

$$x \equiv (3)^{-1} \cdot 12 \pmod{4}$$

$$\Rightarrow x \equiv (3) \cdot 12 \pmod{4}$$

$$x \equiv 36 \pmod{4}$$

$$x \equiv 0 \pmod{4}$$

وهو الحل الكلي

$$x = x_0 + \frac{20}{5}t \quad \text{ذ } t = 0, 1, 2, 3, 4$$

$$x_0 = 0$$

$$x_1 = 4$$

$$x_2 = 8$$

$$x_3 = 12$$

$$x_4 = 16$$

نكتب حل المعادلات الأولى $x \equiv 21 \pmod{30}$ بطريقة ديونانيس

$$x = -21 \Leftrightarrow 9$$

$$x = -11 \Leftrightarrow 19$$

$$x = -1 \Leftrightarrow 29 \quad (29 + 11 = 40)$$

$$29 \equiv -1 \pmod{30}$$

الأسود البسيطة المستمرة المنتهية 2

إن إظهار حلول النماذج في الخطة باستقام فواردية اعتد ساء أو بالقرية
تبع طولية أو متعة صيف يكون المتاح كبيراً
لذا استخدم طريقة السود البسيطة المستمرة المنتهية
القرية السوداء البسيطة المستمرة المنتهية هو كل كسري كسري في النواذيب

$$\frac{A}{B} = a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \frac{1}{\ddots}}}$$

$$\boxed{\mathbb{Z}^+ \ni a_1, a_2, \dots, a_{n-1}, a_n} \quad \mathbb{Z}^+ \ni a_2, a_3, \dots, a_{n-1}, a_n \quad \text{صيف 1}$$

$$\boxed{a_1 \in \mathbb{Z}} \quad \text{صيف 2}$$

وغيره له بـ

$$\frac{A}{B} = \langle a_1, a_2, \dots, a_{n-1}, a_n \rangle$$

والطال ويجز ذلك: أكتب الكسر

$$\frac{32}{19} = 1 + \frac{13}{19}$$

$$\frac{32}{19} = 1 + \frac{13}{19} \quad \boxed{32 = 1 \cdot (19) + 13}$$

$$= 1 + \frac{1}{\left(\frac{19}{13}\right)} = 1 + \frac{1}{1 + \left(\frac{6}{13}\right)} = 1 + \frac{1}{1 + \frac{1}{\left(\frac{13}{6}\right)}} = 1 + \frac{1}{2 + \frac{1}{6}}$$

$$\frac{32}{19} = \langle 1, 1, 2, 6 \rangle$$

بذلك: أكتب الكسر

$$-\frac{5}{4} = -2 + \frac{3}{4}$$

$$= -2 + \frac{1}{\frac{4}{3}} = -2 + \frac{1}{1 + \frac{1}{3}}$$

$$\boxed{-5 = (-2)(4) + 3}$$

$$-\frac{5}{4} = \langle -2, 1, 3 \rangle$$

يصبح العدد (a_k) السبة الجزئية من المرتبة k وإذا توقفنا بالسر عند
السبة الجزئية فنحصل مع التقريب من المرتبة k الذي يبرز له C_k

$$C_1 = a_1$$

$$C_2 = a_1 + \frac{1}{a_2}$$

أي

$$c_3 = a_1 + \frac{1}{a_2 + \frac{1}{a_3}}$$

$$c_k = a_1 + \frac{1}{a_2 + \frac{1}{a_{k-1} + \frac{1}{a_k}}}$$

تمرين 1 إذا كانت لدينا الكسور البسيطة المستمرة $\langle a_1, a_2, a_3, \dots, a_{n-1}, a_n \rangle$ رادفلكا البروزا شريطة

$$p_1 = a_1$$

$$q_1 = 1$$

$$p_2 = a_1 \cdot a_2 + 1$$

$$q_2 = a_2$$

$$p_3 = a_3 \cdot p_2 + p_1$$

$$q_3 = a_3 \cdot q_2 + q_1$$

$$p_i = a_i \cdot p_{i-1} + p_{i-2}$$

$$q_i = a_i \cdot q_{i-1} + q_{i-2}$$

$$p_n = a_n \cdot p_{n-1} + p_{n-2}$$

$$q_n = a_n \cdot q_{n-1} + q_{n-2}$$

فإن التقريب من الرتبة (n) لكسر (c_n) العظمى يساوي $C_n = \frac{p_n}{q_n}$ و $n \geq 1$

تمرين 2 مع أجل $n \geq 2$ ولجميع البروز في المبرمجة السابقة تكون العدة المتتالية صحيحة:

$$p_n \cdot q_{n-1} - p_{n-1} \cdot q_n = (-1)^n$$

تمرين 3 الكسور البسيطة نقول أن $a' = a^*$ هو النقر البشري للعدد الصحيح a بالمتناس m إذا وفقط إذا كان

$$a a^* \equiv 1 \pmod{m} \Leftrightarrow \begin{matrix} \text{in } \mathbb{Z}_m \\ \bar{a} \cdot \bar{a}^* = \bar{1} \end{matrix}$$

يكون للعدد الصحيح a الحشري بالمتناس m إذا وفقط إذا كان $d(a, m) = 1$

$$U(\mathbb{Z}_m) = \{ \bar{a} \in \mathbb{Z}_m : d(a, m) = 1 \}$$

(ه) وفقط ه لي صنفوا تواصيا
توحي مع m

$$(5)' m \mathbb{Z}_5$$

مثال: بالمراسلة القوية للعدد 5

بالمقاس 11

$$\overline{5} = \overline{10} = \overline{15} = \dots$$

هو 0

حل جملة تطابقات خطية

$$b_i x \equiv a_i \pmod{m_i}$$

لتكن جملة التطابقات الخطية

يقول أن العدد الصحيح x حل مشترك لجملة التطابقات إذا تحقق جميع التطابقات اعطاة معاً.

مبرهنة صيني للصين

إذا كانت التطابقات (m_1, m_2, \dots, m_k) أولية نسبية متتالية

فإنه يوجد لجملة التطابقات $x \equiv a_i \pmod{m_i} \quad (i=1, \dots, k)$

حل وحيد بالمقاس $m = m_1 m_2 \dots m_k$

ويعطى بالصيغة التالية:

$$x = [m'_1 M_1 a_1 + m'_2 M_2 a_2 + \dots + m'_k M_k a_k] \pmod{m}$$

$$M_i = \frac{m}{m_i}$$

حيث

$$(m'_i, M_i) \equiv 1 \pmod{m_i} \quad (m'_i, M_i) \text{ بالمراسلة القوية لـ } m_i$$

$$m'_i = (M_i)^{-1} \text{ in } \mathbb{Z}_{m_i}$$

مثال: حل جملة أولية أصغر عدد صحيح يترك بقايا معينة على 6 يساوي 2

وباقى قسمة على 5 يساوي 3 وباقى قسمة على 11 يساوي 7

$$\begin{cases} x \equiv 2 \pmod{6} \\ x \equiv 3 \pmod{5} \\ x \equiv 7 \pmod{11} \end{cases}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 7 \pmod{11}$$

$$m_1 = 6$$

$$m_2 = 5$$

$$m_3 = 11$$

فلا خلاف

$$3+x \equiv 2 \pmod{6}$$

$$x \equiv -1 \pmod{6}$$

$$x \equiv 5$$

ع. نسبيًا ثلث ثلثين وبالتالي يمكن تطبيق برهنة الباقي الصينية (أو نسبية التماثلات ملوليه)

$$m = 6 \cdot 5 \cdot 11 = 330$$

$$M_1 = \frac{330}{6} = 55$$

$$M_2 = \frac{330}{5} = 66$$

$$M_3 = \frac{330}{11} = 30$$

$$m'_1 M_1 \equiv 1 \pmod{6} \Rightarrow m'_1 \cdot 55 \equiv 1 \pmod{6}$$

$$m'_1 \cdot 1 \equiv 1 \pmod{6} \Rightarrow \boxed{m'_1 \equiv 1 \pmod{6}}$$

$$m'_2 M_2 \equiv 3 \pmod{5} \Rightarrow m'_2 \cdot 66 \equiv 3 \pmod{5}$$

$$\boxed{m'_2 \equiv 1 \pmod{5}}$$

$$m'_3 M_3 \equiv 7 \pmod{11} \Rightarrow m'_3 \cdot 30 \equiv 7 \pmod{11}$$

$$m'_3 (8) \equiv 1 \pmod{11} \Rightarrow m'_3 \equiv (8)^{-1} \pmod{11}$$

$$\boxed{8 \cdot 7 = 1}$$

$$\Rightarrow \boxed{m'_3 \equiv 7 \pmod{11}}$$

ونستم يكون الكل (x)

$$x \equiv [1 \cdot 55 \cdot 2 + 1 \cdot 66 \cdot 3 + 7 \cdot 30 \cdot 7] \pmod{330}$$

$$= [110 + 198 + 1470] \pmod{330}$$

$$= [1778] \pmod{330}$$

$$1 \equiv (128) \pmod{330}$$

$$\Rightarrow \boxed{x = 128}$$

نريد التثبت أوله حل التمثيل

$$19x \equiv 1 \pmod{140}$$

طريقة افند نأخذ أوله الخ موزة

طريقة الباقي الصينية

من أول طريقة الباقي الصينية

من أول طريقة الباقي الصينية (140) عوامل أولية ثلثين ثلثين فثلاث مائة (140 = 4 \cdot 5 \cdot 7)

ومن ثم التمثيل بـ 1

$$\left. \begin{array}{l} 19x \equiv 1 \pmod{4} \\ 19x \equiv 1 \pmod{5} \\ 19x \equiv 1 \pmod{7} \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} 3x \equiv 1 \pmod{4} \\ 4x \equiv 1 \pmod{5} \\ 5x \equiv 1 \pmod{7} \end{array} \right\} \Rightarrow$$

$$\left. \begin{array}{l} x \equiv (3)^{-1} \cdot 1 \pmod{4} \\ x \equiv (4)^{-1} \cdot 1 \pmod{5} \\ x \equiv (5)^{-1} \cdot 1 \pmod{7} \end{array} \right\} \Leftrightarrow \left. \begin{array}{l} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{7} \end{array} \right\}$$

$$\left. \begin{array}{l} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{7} \end{array} \right\}$$

$$\left. \begin{array}{l} x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \\ x \equiv 3 \pmod{7} \end{array} \right\}$$

نأخذ بـ 140 موزة
أولها الخ موزة

طريقة

مبرهنة فيرما الصغيرة

إذا كانت p عدداً أولياً لا يقسم العدد الصحيح a ،
فغند $a^{p-1} \equiv 1 \pmod{p}$ و $a(p-1) = 1$

$$a^p \equiv a \pmod{p}$$

$$(Z_p, +, \cdot)$$

البنية

$$Z_p = \{0, 1, \dots, p-1\}$$

$$U(Z_p) = \{1, 2, \dots, p-1\}$$

وهي

$$|U(Z_p)| = p-1$$

وهي مجموعة لا غنائية رتاً فيها كوناً

$$\bar{a} \in U(Z_p) \Rightarrow (\bar{a})^{p-1} = \bar{1}$$

$$\Rightarrow (a^{p-1}) = 1$$

$$\bar{a} \in U(Z_p) \Rightarrow \text{عندئذ } \text{dep}(a) = 1$$

$$(\bar{a})^{p-1} = \bar{1} \Rightarrow (a^{p-1}) = 1$$

بالانتقال إلى المتطابقات فنحصل على أن

$$a^{p-1} \equiv 1 \pmod{p}$$

ننتج إذا كانت p عدداً أولياً وكون a عدداً صحيحاً فغند

$$a^p \equiv a \pmod{p}$$

مبرهنة فيرما الصغيرة

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^p \equiv a \pmod{p}$$

$$p | a$$

$$a \equiv 0 \pmod{p}$$

$$p | a$$

$$a^p \equiv 0 \pmod{p} \Leftrightarrow p | a^p$$

$$a^p \equiv a \pmod{p}$$

وهو المطلوب

$$\text{plac}(a^{p-1}) \quad \text{plac}(a) \Rightarrow a^p \equiv a \pmod{p}$$

وهو المطلوب

نقطة إذا كانت $a \equiv a \pmod{n}$ فليس بالضرورة أن يكون n أولياً (العكس صحيح)

$$5^{10} \equiv 1 \pmod{11} \quad \text{بقوة للبيت 9 ثبتت}$$

$$11 \mid (5^{10} - 1) \quad \text{البيت 11 كى 11 يتبع}$$

$$(5^{10}) \equiv 1 \pmod{11}$$

نمثلة إذا كانت p و q عددين أوليين مختلفين فكان

$$a^p \equiv a \pmod{q}$$

$$a^q \equiv a \pmod{p}$$

فكان $\text{lcm}(p, q) = 1$ عندئذ:

$$a^{pq} \equiv a \pmod{p \cdot q}$$

نمثلة (P) حلل العدد 341 بطريقة فريما.

$$2^{340} \equiv 1 \pmod{341} \quad \text{ثبتت أن (C)}$$

$$2^{341} \equiv 2 \pmod{341}$$

العدد الذي في هذا الشكل 2^n $n \in \mathbb{Z}$
 فبالطولية التي تحقق السرعة

$$2^n = 2 \pmod{n}$$

تدعى أسيباً أوليات (أوليات كاذبة)
 والعدد (341) هو أول عدد يقبله أولي
 رتبة (61) (561)

انتهت المحاضرة